National Aeronautics and
Space Administration

NOT MEASUREMENT
SENSITIVE

NASA-STD-2804-O
Effective August 9, 2011

MINIMUM INTEROPERABILITY SOFTWARE SUITE

NASA TECHNICAL STANDARD

FOREWORD

This standard is approved for use by NASA Headquarters and all NASA centers and is intended to provide a common framework for consistent practices across NASA programs.

The material covered in this standard is governed and approved by the NASA Information Technology Management Board. Its purpose is to define the baseline software suite necessary to support interoperability both between NASA end user computers and within the NASA operating environment. The standard establishes Client Reference Configurations, Operating System Standards, and Compliance Dates for computers running Microsoft Windows, Apple Mac OS, and various Linux and UNIX operating systems. Adherence to this standard ensures compliance with Federal requirements for desktop computers, laptops, and other end user devices.

Requests for information, corrections, or additions to this standard should be directed to the John H. Glenn Research Center at Lewis Field (GRC), Emerging Technology and Desktop Standards Group (ETADS), MS 142-4, Cleveland, OH, 44135 or to *desktop-standards@lists.nasa.gov*. This standard may be viewed and downloaded, free of charge, from the NASA Emerging Technology and Desktop Standards web site:
http://etads.nasa.gov/current/2804.pdf

/signature on file/

Linda Cureton
Chief Information Officer

This Page Left Blank Intentionally

Table of Contents

1 SCOPE

1.1 Purpose

This standard defines the baseline software suite necessary to support interoperability both between NASA end user computers and within the NASA operating environment. The standard establishes Client Reference Configurations, Operating System Standards, and Compliance Dates for computers running Microsoft Windows, Apple Mac OS, and various Linux and UNIX operating systems. Adherence to this standard ensures compliance with Federal requirements for desktop computers, laptops, and other end user devices.

1.2 Applicability

Center CIOs will ensure that all NASA employees at their respective centers have access to an interoperable workstation that is equipped with a minimum software suite that meets the standards listed in Section 3 below.

The Client Reference Configuration (CRC) establishes required functionality and required products necessary to meet that functionality. Future procurements intended to address this functionality are restricted to the products defined in the CRC. Existing licenses for other products may not be renewed. Products will be added, replaced, or removed as appropriate to address agency interoperability requirements.

1.3 Waivers

This technical standard is governed by Enterprise Architecture Function as defined in Section 1.2.1.3 of NPR 2800.1B *Managing Information Technology.* Adherence to this standard ensures compliance with the future state architecture as described in NPR 2830.1 *NASA Enterprise Architecture Procedures.*

The Emerging Technology and Desktop Standards group, in cooperation with the End User Services Service Executive and the Chief Enterprise Architect, will evaluate and process waivers to this standard as appropriate. Waiver requests will include:

1) the reason the waiver is required,
2) justification for the waiver, and
3) a proposed date by which compliance with the standard will be met.

Waivers will be granted by the NASA CIO or at his/her discretion responsibility will be delegated to the Center or Mission Directorate CIO.

2 ACRONYMS AND DEFINITIONS

2.1 Acronyms

ACES	Agency Consolidated End-User Services
ASCS	Agency Security Configuration Standards
ASUS	Agency Security Update Service
CA	Certificate Authority
CIO	Chief Information Officer
CIS	Center for Internet Security
CRC	Client Reference Configuration
CSS	Cascading Style Sheets

DAR	Data at Rest (encryption)
DSI	Desktop Smartcard Integration
ETADS	Emerging Technology and Desktop Standards
FDCC	Federal Desktop Core Configurations
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FPKI	Federal Public Key Infrastructure
GnuPG	GNU Privacy Guard
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
ICA	Independent Computing Architecture
ICAM	Identity Credential Access Management
IE	Internet Explorer
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ISO	International Standards Organization
ITAR	International Traffic in Arms Regulations
IMAP	Internet Message Access Protocol
LCS	Microsoft Office Live Communication Server
LTS	Long-term Support
MAPI	Messaging Application Programming Interface
MIME	Multipurpose Internet Mail Extension
NCTR	NASA Client Trust Reference
NEF	NASA Electronic Forms
NFCE	NASA Firefox Configuration Extension
NIST	National Institute of Standards and Technology
NOCA	NASA Operational Certificate Authority
NOMAD	NASA Operational Messaging and Directory Service
NSS	Network Security Services
OASIS	Organization for the Advancement of Structured Information Standards
OCIO	Office of the Chief Information Officer
OCS	Microsoft Office Communications Server
PDF	Portable Document Format
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RFC	Request for Comments
SBU	Sensitive But Unclassified
SCAP	Security Content Automation Protocol
SFTP	Secure File Transfer Protocol
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMTP	Simple Mail Transport Protocol
SSH	Secure Shell Protocol
SSL	Secure Sockets Layer
S/MIME	Secure/Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
USGCB	United States Government Configuration Baseline
VPAT	Voluntary Product Accessibility Templates
W3C	World Wide Web Consortium

XHTML	eXtensible HyperText Markup Language
XML	Extensible Markup Language
XMPP	Extensible Messaging and Presence Protocol

2.2 Definitions

2.2.1 Basic Interoperability

Interoperability is the ability to obtain consistent and deterministic results within a specific platform (operating system software, minimum hardware, required and optional software) as well as between platforms (Microsoft, OS X, Linux, Unix) based on the established standards.

2.2.2 Desktop Computer

The term desktop computer is used generically to refer to traditional desktop systems, as well as laptop computers, notebooks, tablets, engineering workstations, and similar platforms that are utilized to provide basic interoperability.

2.2.3 Support for Basic Interoperability

Systems supporting basic interoperability are defined as desktop computers used to exchange information electronically by end users that require any of the functionality listed in Section 3.3, Client Reference Configurations.

3 DETAILED REQUIREMENTS

3.1 Architectural Compliance Requirements

NASA has baselined and approved the NASA Integrated Information Technology Architecture[1]. The architecture is predicated on:

- The selection of standards for a broad and cost-effective infrastructure using commercial off-the-shelf and well-supported open source products to the greatest extent practical
- Interoperability both within and external to NASA
- Flexibility for future growth
- Consistency with generally accepted consensus standards as much as feasible

Among these objectives, ensuring interoperability is one of NASA's most critical issues related to information technology. In many cases, it is in NASA's best interest to specify commercial products as standards for an interoperable implementation of a particular set of related and integrated functions. The products themselves often include additional functionality or proprietary extensions not specified by this standard. While these products can be used to create higher-level interoperability solutions, these solutions may not be recognized within the context of the NASA interoperability environment and may be deprecated without warning by future revisions to this standard. Users of this standard are advised to apply appropriate caution when implementing proprietary or non-standard extensions, features and functions that go beyond the explicitly stated standard functionality.

1 NASA-STD-2814A, *NASA Integrated Information Technology Architecture—Technical Framework*

3.2 Agency Security Configuration Standards

The NASA Office of the Chief Information Officer (OCIO) establishes Agency Federal Information Security Management Act (FISMA) compliance goals and reporting requirements for NASA systems, through the use of NASA System Security Baselines, managed by the Agency Security Configuration Standards (ASCS) project. OCIO policy requires deployment of the NASA ASCS system configurations to all systems.

The NASA ASCS system baselines are developed from various sources such as the National Institute of Standards and Technology (NIST) Security Content Automation Program (SCAP) checklists for systems which have SCAP settings available. Center for Internet Security (CIS) Benchmarks provide the basis for other operating systems and applications, with review and potential adjustment for the NASA environment by the ASCS project.

NASA Baseline security configurations for each operating system and applicable software listed in this standard can be obtained at:

http://etads.nasa.gov/ASCS/

Centers wishing informed local consultation should contact their ASCS Point of Contact, listed here:

http://etads.nasa.gov/ASCS/Communications.shtml

or consult the ASCS web site for additional information.

3.3 Client Reference Configurations

To address application, data, and infrastructure interoperability, and ensure compliance with federally mandated desktop computer configuration settings, the software functionality, applications, interface standards, configuration settings, versions, and deployment settings established by this standard are definitive.

Client Reference Configurations (CRC) are included for each operating system, with specific version and required configurations listed as appropriate. Interface standards are included to guide service providers and system integrators.

The Client Reference Configurations define the baseline upon which desktop service providers can define common enterprise images for all interoperable desktops computers. All IT initiatives funded or endorsed by the NASA OCIO account for systems that conform to the Client Reference Configurations. Application service providers and software developers can use the reference configurations to assist with integration and acceptance testing.

The NASA Emerging Technology and Desktop Standards group is working to ensure interoperability at the highest possible revision of products included in the Client Reference Configurations. Applications that meet these interface standards while providing improved end user experience, mitigating security risks, reducing support costs, or offering other tangible improvements may be submitted to desktop-standards@lists.nasa.gov for consideration in future revisions to these standards.

3.3.1 Client Reference Configuration for Windows XP

Client Reference Configuration for Windows XP					
Functionality	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Effective Date**
Operating System	Windows XP Professional		NASA System Baseline Configuration settings2	Service Pack 3 with all security patches	September 30, 2008
	Windows XP Professional X64 Edition		NASA System Baseline Configuration settings3 KB968730 Hotfix4	Service Pack 2 with all security patches	April 1, 2009
Firewall	Windows Firewall		NASA System Baseline Configuration settings5	XP/SP3	September 30, 2008
Smartcard Middleware	ActivIdentity ActivClient	NIST SP 800-73 Part 3	See section 3.6.1	XP 32-bit is 6.2.x XP x64 is 6.1.x	September 7, 2010
Data at Rest , Full Disk Encryption	McAfee Endpoint Encryption		Configured to use central policy and key escrow service See section 3.5.5.1	5.2.x	April 1, 2009
Content Encryption	Entrust ESP	S/MIME		9.1.x	September 7, 2010
Secure Email	Entrust ESP	S/MIME		9.1.x	September 7, 2010
Trust Anchor Management	See Section 3.6	FPKI	See Section 3.6	3.1.x	August 9, 2011
Anti-Virus	Symantec Endpoint Protection		Enterprise update server	11.0.x	September 7, 2010
Anti-Malware	Symantec Endpoint Protection		Enterprise update server	11.0.x	June 24, 2008
Patch Reporting	KBOX	KACE Proprietary	See section 3.5.4	5.0.x	September 7, 2010
Web Browser	Mozilla Firefox	W3C and industry standards, including the following: HTML 4.01, XHTML 1.1, CSS 2.1, HTML5, CSS 3, WebFonts, ECMAscript, Java applet support, TLS 1.2, SSLv3	See sections 3.6	5.0x	August 9, 2011
	Microsoft Internet Explorer		NASA System Baseline Configuration settings. Also see sections 3.6	8.0.x	September 7, 2010

2 Check http://etads.nasa.gov/ASCS/ for current configurations

3 Check http://etads.nasa.gov/ASCS/ for current configurations

4 Supplemental hotfix to support SHA-2 encryption algorithms

5 Check http://etads.nasa.gov/ASCS/ for current configurations

Client Reference Configuration for Windows XP					
Functionality	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Effective Date**
Office Automation	Microsoft Office (Professional Edition with Outlook)			2010	December 1, 2010
Word Processing	Microsoft Word	Office Open XML document format	Configure to use Office Open XML file format by default	2010	December 1, 2010
Spreadsheet	Microsoft Excel	Office Open XML document format	Configure to use Office Open XML file format by default	2010	December 1, 2010
Presentation	Microsoft PowerPoint	Office Open XML document format	Configured to use Office Open XML file formats by default	2010	December 1, 2010
Electronic Mail	Microsoft Outlook	NASA-STD-2815, IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	2010	December 1, 2010
Calendaring	Microsoft Outlook as implemented by NOMAD	iCalendar (RFC 5545)6		2010	December 1, 2010
Instant Messaging	Office Communicator	SIP	Enterprise LCS Settings as implemented by NOMAD Pidgin-sipe LCS/OCS plugin	2007 R2	July 1, 2011[7]
	Pidgin	XMPP	NASA Jabber Service Pidgin-sipe LCS/OCS plugin	2.9.x	June , 2009
PDF Viewer	Adobe Reader X	PDF		10.0.x	August 9, 2011
Java	Java run-time environment		With all security patches	Java 6	October 1, 2008
Audio/video players (all are required	Apple QuickTime Player	Various Multimedia	Default for QuickTime formats	7.6.x	June 24, 2008
	Adobe Player	Flash SWF		10.3.x	August 9, 2011
	Microsoft Windows Media Player	Windows Media Files	Default for all supported formats	11.0.x	June 24, 2008
	Silverlight	Various Multimedia		4.0.x	September 7, 2010
	Apple iTunes	Various Multimedia		10.4.x	August 9, 2011
Access to centrally served Windows applications	Citrix ICA Client	Citrix ICA ProtocolXenApp Plugin		12.1x	August 9, 2011

6 This standard provides limited interoperability

7 Date specified by NOMAD

Client Reference Configuration for Windows XP					
Functionality	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Effective Date**
Electronic Forms	FileNet Desktop e-Forms	See Section 3.7	NASA Distribution Center	4.2	June 24, 2008
Video Conferencing	Secure Virtual Team Meeting		https://nasa.webex.com/		August 2010

3.3.2 Client Reference Configuration for Windows 7

Client Reference Configuration for Windows 7					
Functionality	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Effective Date**
Operating System	Windows 7 Enterprise or Ultimate		NASA Baseline Security settings8	SP1	August 9, 2011
	Windows 7 Enterprise or Ultimate X64 Edition		NASA Baseline Security settings9	SP1	August 9, 2011
Firewall	Windows Firewall		NASA Baseline Security settings10		September 7, 2010
Smartcard Middleware	ActivIdentity ActivClient	NIST SP 800-73 Part 3	See section 3.6.1	6.2.x	September 7, 2010
Data at Rest, Full Disk Encryption	McAfee Endpoint Encryption		Configured to use central policy and key escrow service See section 3.5.5.1	5.2.x	September 7, 2010
Content Encryption	Entrust	S/MIME		9.1.x	September 7, 2010
Secure Email	Entrust Desktop Solution	S/MIME		9.1x	September 7, 2010
Trust Anchor Management	See Section 3.6	FPKI	See Section 3.6	3.1.x	August 9, 2011
Anti-Virus	Symantec Endpoint Protection		Enterprise update server	11.0.X	September 7, 2010
Anti-Malware	Symantec Endpoint Protection		Enterprise update server	11.0.X	September 7, 2010
Patch Reporting	KBOX	Proprietary		5.2.x	September 7, 2010
Web Browser	Mozilla Firefox	W3C and industry standards, including the following: HTML 4.01, XHTML 1.1, CSS 2.1, HTML5, CSS 3, WebFonts, ECMAscript, Java applet support, TLS 1.2, SSLv3	See sections 3.6	5.0.x	August 9, 2011
	Microsoft Internet Explorer		NASA FDCC Baseline Configuration settings. Also see sections 3.6	9.0.x	February 1, 2012
Office Automation	Microsoft Office (Professional Edition with Outlook)			2010	December 1, 2010

8 Check http://etads.nasa.gov/ASCS/ for current configurations

9 Check http://etads.nasa.gov/ASCS/ for current configurations

10 Check http://etads.nasa.gov/ASCS/ for current configurations

Client Reference Configuration for Windows 7					
Functionality	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Effective Date**
Word Processing	Microsoft Word	Office Open XML document format	Configure to use Office Open XML file format by default	2010	December 1, 2010
Spreadsheet	Microsoft Excel	Office Open XML document format	Configure to use Office Open XML file format by default	2010	December 1, 2010
Presentation	Microsoft PowerPoint	Office Open XML document format	Configure to use Office Open XML file formats by default	2010	December 1, 2010
Electronic Mail	Microsoft Outlook	NASA-STD-2815, IMAP4, SMTP, IMAP over SSL/TLS, MAPI over HTTPS	Configured for access to NOMAD	2010	December 1, 2010
Calendaring	Microsoft Outlook as implemented by NOMAD	iCalendar (RFC 5545)11		2010	December 1, 2010
Instant Messaging	Communicator	SIP	Enterprise LCS Settings as implemented by NOMAD Pidgin-sipe LCS/OCS plugin	2007 R2	August 9, 2011[12]
	Pidgin	XMPP	NASA Jabber Service Pidgin-sipe LCS/OCS plugin	2.9.x	August 9, 2011
PDF Viewer	Adobe Reader X	PDF		10.0.x	August 9, 2011
Java	Java run-time environment		With all security patches	Java 6	September 7, 2010
Audio/video players (all are required)	Apple QuickTime Player	Various Multimedia	Default for Quicktime formats	7.6.x	September 7, 2010
	Adobe Flash Player	Flash SWF		10.3.x	August 9, 2011
	Microsoft Windows Media Player	Windows Media Files	Default for all supported formats	12.0.x	September 7, 2010
	Silverlight	Various Multimedia		4.0.x	September 7, 2010
	Apple iTunes	Various Multimedia		10.4.x	September 7, 2010
Access to centrally served Windows applications	Citrix ICA Plugin	Citrix ICA ProtocolXenApp Plugin		12.1.x	September 7, 2010
Electronic Forms	FileNet Desktop e-Forms	See Section 3.7	NASA Distribution Center	4.2	September 7, 2010

11 This standard provides limited interoperability

12 Date specified by NOMAD

Client Reference Configuration for Windows 7					
Functionality	**Application**	**Interface Standard**	**Required Settings**	**Version**	**Effective Date**
Video Conferencing	Secure Virtual Team Meeting		https://nasa.webex.com/		September 7, 2010

3.3.3 Client Reference Configuration for Mac OS X

Client Reference Configuration for Mac OS X					
Functionality	**Application**	**Interface Standards**	**Required Settings**	**Version**	**Effective Date**
Operating System	Mac OS X		CIS Benchmarks	10.6.x	April 1, 2010
Firewall	Apple Firewall		Allow essential services Enable firewall logging Enable Stealth Mode[13]		April 1, 2009
Smartcard Middleware	Bundled with OS		See Section 3.6.1		April 1, 2010
PKI	Entrust Secure Desktop for Mac (SDM)	S/MIME	NASA PKI Team specified settings	8.0	July 2, 2010
Trust Anchor Management	See Section 3.6	FPKI	See Section 3.6	3.1.x	August 9, 2011
Anti-Virus	Symantec Endpoint Protection			11.0.x	August 9, 2011
Anti-Malware	Symantec Endpoint Protection			11.0.x	August 9, 2011
Data at Rest Encryption			Configured to use central policy and key escrow service See section 3.5.5.1	Not Available	Not Available
Home Folder Encryption	FileVault	Apple Proprietary		Bundled	September 7, 2010
Web Browser	Mozilla Firefox	W3C and industry standards, including the following: HTML 4.01, XHTML 1.1, CSS 2.1, HTML5, CSS 3, WebFonts, ECMAscript, Java applet support, TLS 1.2, SSLv3	See sections 3.6	5.0x	August 9, 2011
	Apple		See sections 3.6	5.1.x	July 2011
Java	Java Run-time Environment		With all security patches	Java 6 bundled	October 1, 2008
Office Automation	Microsoft Office 2011 for Mac			2011	April 1, 2011
Word Processing	Microsoft Word 2011 for Mac	Office Open XML document format	Configure to use Office Open XML file format by default	14.0.x	April 1, 2011

13 Vendor terminology for these settings

Client Reference Configuration for Mac OS X					
Functionality	**Application**	**Interface Standards**	**Required Settings**	**Version**	**Effective Date**
Spreadsheet	Microsoft Excel 2011 for Mac	Office Open XML document format	Configure to use Office Open XML file format by default	14.0.x	April 1, 2011
Presentation	Microsoft PowerPoint 2011 for Mac	Office Open XML document format	Configure to use Office Open XML file formats by default	14.0.x	April 1, 2011
Electronic Mail	Microsoft Outlook 20011for Mac	NASA-STD-2815, IMAP4, SMTP, IMAP over SSL/TLS	Configured for access to NOMAD	14.0.x	April 1, 2011
	Apple Mail		Integration with NOMAD limited to email only	4.5.x	July ,2011
Calendaring	Microsoft Outlook 2011for Mac as implemented by NOMAD	iCalendar (RFC 5545)14	Configured for access to NOMAD	14.0.x	April 1, 2011
	Apple iCal	iCalendar (RFC 5545)15	Configured for access to NOMAD	4.0.x	July 2010
Instant Messaging	Mac Messenger	SIP	Enterprise LCS Settings as specified by NOMAD	7.0.x	July 1, 2011[16]
	Apple iChat	XMPP	NASA Jabber Service settings	Bundled	June 24, 2008
Patch Reporting	KBOX	KACE Proprietary	See section 3.4.4	5.2.x	September 7, 2010
Audio/video players (all are required)	Apple QuickTime Player	Various Multimedia		10.0.x	August 9, 2011
	Adobe Flash Player	Flash SWF		10.3.x	July ,2011
	Telestream Flip4Mac WMV	Windows Media	Default for Windows Media	2.3.x	June 24, 2008
	SilverLight	Various Multimedia		4.0.x	July 1, 2010
	Apple iTunes	Various Multimedia	Default for all supported formats	10.4.x	August 9, 2011
PDF Viewer	Apple Preview			5.0.x	April 1, 2010
Access to centrally served Windows applications	Citrix ICA Client	Citrix ICA Protocol XenApp Plugin		11.2.x	July ,2011

14 This standard provides limited interoperability

15 This standard provides limited interoperability

16 Date specified by NOMAD

Client Reference Configuration for Mac OS X					
Functionality	**Application**	**Interface Standards**	**Required Settings**	**Version**	**Effective Date**
Electronic Forms	FileNet Desktop e-Forms	See Section 3.7	NASA Distribution Center	4.2	June 24, 2008
Video Conferencing	Secure Virtual Team Meeting		https://nasa.webex.com/		August 2010

3.3.4 Client Reference Configuration for Linux

Client Reference Configuration for Linux					
Functionality	**Application**	**Interface Standards**	**Required Settings**	**Version***	**Effective Date**
Operating System	Red Hat Enterprise Linux Desktop with Workstation option		CIS Benchmarks	5.3 or later	June 24, 2008
	Ubuntu		CIS Benchmarks	10.0.4	July 2010
Firewall	Bundled		Control inbound and outbound connections enabled by default	Bundled	June 24, 2008
Smartcard Middleware	ActivIdentity ActivClient		See Section 3.6.1	32-bit 3.0.x 64-bit Unsupported	September 2010
Secure Email	Thunderbird	S/MIME	Use exported NOCA certificates	3.0.x	September 7, 2010
Trust Anchor Management	See Section 3.6	FPKI	See Section 3.6	3.1.x	August 9, 2011
Anti-Virus	Symantec Antivirus for Linux			1.0.x	July 2010
Data at Rest Encryption	McAfee Endpoint Encryption		Configured to use central policy and key escrow service	Not Available	Not Available
Patch Reporting	PatchLink (Update)	Lumension Proprietary	Configuration for Server info	6.4.x	June 30, 2008
	KBOX	KACE Proprietary	See Section 3.5.4	5.2.x	September 7, 2010
Web Browser	Mozilla Firefox	W3C and industry standards, including the following: HTML 4.01, XHTML 1.1, CSS 2.1, HTML5, CSS 3, WebFonts, ECMAscript, Java applet support, TLS 1.2, SSLv3		5.0.x	July 2010

Client Reference Configuration for Linux					
Functionality	**Application**	**Interface Standards**	**Required Settings**	**Version***	**Effective Date**
Office Automation	LibreOffice.org[17]	OASIS Open Document Format for Office Applications (OpenDocument		3.3.x	August 9, 2011
Word Processing	LibreOffice[18] Writer	OASIS Open Document Format for Office Applications (OpenDocument	Configure to use Office Open XML file format by default	3.3.x	August 9, 2011
Spreadsheet	LibreOffice[19] Calc	OASIS Open Document Format for Office Applications (OpenDocument	Configure to use Office Open XML file format by default	3.3.x	August 9, 2011
Presentation	LibreOffice[20] Impress	OASIS Open Document Format for Office Applications (OpenDocument	Configure to use Office Open XML file format by default	3.3.x	August 9, 2011
Electronic Mail	Mozilla Thunderbird	NASA-STD-2815, IMAP4, SMTP, IMAP over SSL/TLS	Configured for access to NOMAD	3.1.x	August 9, 2011
Calendaring	NOMAD Outlook Web Access	iCalendar (RFC 5545)21, HTTPS	Web Browser	2.x	June 24, 2008
Instant Messaging	Not Available	SIP	Enterprise LCS Settings as specified by NOMAD Pidgin-sipe LCS/OCS plugin		
	Pidgin	XMPP	NASA Jabber Service settings	2.9.x	June 24, 2008
Java	Java run-time environment		With all security patches	Java 6	June 24, 2008
Audio/video player	MPlayer	Multimedia	Default for supported formats	1.0	June 24, 2008
	Adobe Flash Player			10.3.x	August 9, 2011
PDF Viewer	Adobe Reader			9.3.x	September 7, 2010

17 Open Office may be used for Red Hat Linux clients

18 Open Office may be used for Red Hat Linux clients

19 Open Office may be used for Red Hat Linux clients

20 Open Office may be used for Red Hat Linux clients

21 This standard provides limited interoperability

Client Reference Configuration for Linux					
Functionality	**Application**	**Interface Standards**	**Required Settings**	**Version***	**Effective Date**
Access to centrally served Windows applications	Citrix ICA Client	Citrix Receiver for Linux		11.1.0.x	August 9, 2011
Electronic Forms	FileNet Desktop E-Forms	See Section 3.7	Citrix ICA		
Video Conferencing	Secure Virtual Team Meeting		https://nasa.webex.com/		August 2010

* When the vendor provides bundled support for applications included in the CRC, the vendor-provided and supported versions should supersede those of the CRC

3.4 Operating System Standards, Timelines, and Compliance Dates

3.4.1 Microsoft Windows XP

All Windows XP systems must meet the NASA System Baseline configurations, which ensure compliance with Federal Desktop Core Configuration (FDCC) requirements.

Windows XP must be removed from all NASA systems by October 2013.

3.4.1.1 Microsoft Windows XP 64-bit

Windows XP Professional x 64 Edition is specified as the standard version of Windows 64 bit for the agency interoperable computing environment and is subject to the Windows XP Client Reference Configuration.

Windows XP Professional x 64 Edition must be removed from all NASA systems by October 2013.

3.4.2 Microsoft Windows Vista

Microsoft Windows Vista shall not be deployed.

Vista must be removed from all NASA systems by October 2013.

3.4.3 Microsoft Windows 7

All Windows 7 systems must meet the NASA Baseline Security Configurations Settings, which ensure compliance with United States Government Configuration Baseline (USGCB) requirements.

Microsoft Windows 7 – Enterprise and Ultimate editions only – are approved for deployment. The 64–bit version of Microsoft Windows 7 shall be deployed to all new and refreshed (upgraded) systems. 32–bit versions of Microsoft Windows 7 may be installed if necessary to support non–64 bit capable applications.

Existing Windows XP and Vista systems shall be upgraded to either the 64–bit version of Windows 7 or the 32–bit version depending on hardware capability and software dependency.

Windows 7 shall be required on all Windows systems by October 2013.

3.4.4 Mac OS X

Mac OS X 10.6 (Snow Leopard) is the currently supported operating system on all Intel based interoperable Macintosh systems. . At the time of this writing, Mac OS X 10.6.7 is the current maintenance release. Mac OS X 10.6 shall be installed on all Intel based Macs by June 1, 2011. Older versions should be removed from the environment. As always, the operating system must be kept up-to-date with vendor patches.

Mac OS X 10.6 shall be required on all Intel based Macs by June 1, 2011.

OS X 10.7 (Lion) was released July 20, 2011. Evaluation and interoperability testing was not completed in time for inclusion in this version of the standard. A deployment timeline will be established for general deployment when interoperability testing is complete.

While OS X 10.7 is not approved for general deployment, to facilitate access to the most recent Apple systems, it is approved for use when required by the hardware. Interoperability caveats apply. Contact ETADS for a full list of open issues.

3.4.5 Linux

Linux systems with no need for interoperability need not comply with the interoperability requirements in this standard. Such systems would include special-purpose computers such as name servers, compute servers, data acquisition systems, special software development workstations, or other components of the overall computing infrastructure.

Several product standards are not available for any Linux or UNIX system. In order to comply with this standard, interoperable desktops must have some way to access these products. It is recommended to use the Citrix ICA client to connect to a Microsoft Windows application server.

Two Linux distributions are supported for use on interoperable desktops:

Red Hat Enterprise Linux Desktop 5 with Workstation option:

https://www.redhat.com/rhel/desktop/

Ubuntu 10.04 LTS (Long-term support)

http://www.ubuntu.com/

All new and refreshed Linux systems must run one of the two supported Linux distributions. SuSE Linux Enterprise Desktop has been removed from the standard. SuSE Linux users should be migrated to one of the two supported Linux distros at their earliest convenience. SuSE Linux should be removed from the environment by January 2012.

3.4.6 UNIX

The following UNIX systems are supported in the NASA interoperable computing environment. Generally, both the current version and prior version of the operating system are acceptable. However, the older version of the operating system must continue to be supported by the vendor, and like all systems, must be kept current with security patches.

3.4.6.1 Oracle Solaris/SPARC, x86, and x86-64

Solaris is at version 11. Information about supported Solaris releases may be found at:

http://www.oracle.com/us/products/servers-storage/solaris/index.html - releases

3.4.6.2 IBM AIX/POWER

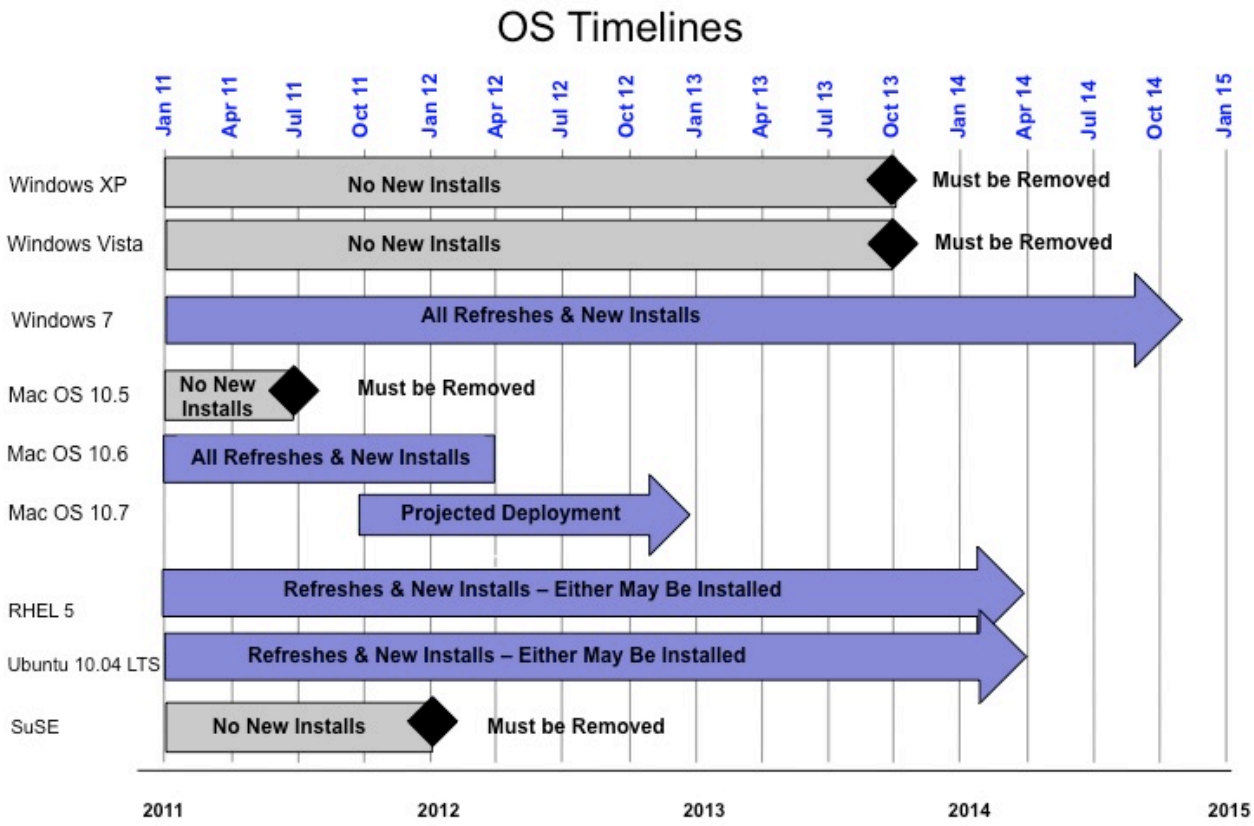
AIX 7 is current. AIX versions are described at:

http://www-03.ibm.com/systems/power/software/aix/index.html

3.4.6.3 HP HP-UX/PA-RISC

HP-UX 11i v3 is current. The HP-UX 11i web page is at:

http://h71028.www7.hp.com/enterprise/w1/en/os/hpux11i-overview.html



3.5 Additional Client Reference Configuration Guidance

3.5.1 Office Automation Applications

The default document format for Microsoft Office, and LibreOffice is the ISO Standard Office Open XML format.

As of December 2011, all interoperable Microsoft Windows systems are required to run the 32–bit version of Office 2010 Standard Edition (or better) regardless of processor architecture. The 64–bit version of Office 2010 may be deployed as a point solution, though interoperability problems will likely persist and be uncorrectable.

Microsoft Office 2011 for Mac (Standard Edition) was approved for use December 1, 2010 and is required on all interoperable Mac OS X systems. A Mac version of Outlook replaces Entourage. Note: Office 2011 reinstates support for Visual Basic Applications.

LibreOffice replaces OpenOffice as the default Office product for Linux platforms. OpenOffice was acquired by Oracle in September 2010 and several members of the OpenOffice.org project formed a new group to continue development of an open software office automation product suite. LibreOffice 3.3 is approved for deployment and use on all Linux platforms. Documents created with Microsoft Office do not always render perfectly in LibreOffice, and vice versa.

3.5.2 Electronic Messaging

NASA has implemented an enterprise-wide electronic messaging service known as NOMAD. This service provides integrated email, calendaring, scheduling, contact management, and instant messaging. All interoperable desktops are required to be configured to access this environment.

Note that while NOMAD is based upon open standards and can support stand-alone email clients that adhere to the defined interface standards of the Client Reference Configurations, utilizing such clients limits end user interoperability, may not be supported by NOMAD, and may result in future inability to participate in the enterprise messaging environment.

Supported Messaging Clients

Windows: Microsoft Outlook

Mac OS X: Microsoft Outlook and Apple Mail

Linux: Mozilla Thunderbird

Apple Mail now supports the NOMAD calendar and scheduling environment but does have some integration issues. The choice of client on Mac OS X depends upon the required functionality. In some cases, Microsoft Outlook is more appropriate (for instance, when delegation functionality is required). In other cases Apple Mail and iCal with Address Book are suitable.

Additional clients which conform to the interface standards may be used as point solutions where interoperability might otherwise not be available.

The selection of mail clients will continue to promote secure access to commercial and partner email services in support of extra-Agency (non-NOMAD) collaborative activities.

3.5.3 Web browser

Both Microsoft and Mozilla have stated that several major browser revisions can be expected before the end of calendar year 2011. To avoid inefficiencies and interoperability issues, NASA must adjust to the rapid pace of browser enhancements resulting in new versions from the browser vendors. Web authors, application providers, system integrators, etc., should ensure that their web sites are validated against W3C Markup Validation Service[22] and discontinue the use of checking client browsers for specific versions before granting access.

NASA's approach to providing interoperable browsers is to support the operating system default browser plus one open software browser that adheres closely to W3C standards. This results in Internet Explorer and Firefox on Windows systems, Safari and Firefox on Macs, and Firefox on Linux systems.

22 http://validator.w3.org/

For Internet Explorer, Firefox, and Safari, NASA will maintain support for the most recent production version and the version immediately preceding it.

Browsers should be configured with the Agency approved list of trust anchors as found in the NASA Client Trust Reference (NCTR). Some browsers will require additional setting, also found at the NCTR site.

http://etads.nasa.gov/DCS/ClientTrustReference.shtml

Browsers should be configured per Desktop ICAM Integration configuration requirements as shown on

https://etads.nasa.gov/DII/CR

For additional information see section 3.6.1 Desktop ICAM Integration

The following table summarizes the timeline for browser support within NASA:

3.5.3.1 Browser Support Timeline Table

Browser	Vendor Release	NASA Support Begins	NASA Support Ends	Comments
IE7	October 2006	September 2010	October 2013	Windows XP Only
IE8	March 2009	September 2010	October 2013	Windows XP
	March 2009	September 2010	July 2012	Windows 7
IE9	March 2011	February 2012		No support for XP
IE10	June 2011			Platform Preview 2
Firefox 3	December 2008	September 2010	October 2011	3.6.16 or later.
Firefox 4	March 2011			Do not deploy
Firefox 5	July 2011	August 2011	with release of Firefox 6	
Firefox 6	April 2011 August 2011			
Firefox 7	May 2011 September 2011			
Firefox 8	July 2011 November 2011			
Safari 4	February 2009	June 2009	August 2011	Safari 4 should be removed from the environment
Safari 5	June 2010	September 2010		
Chrome 10	March 2011			Not supported; undergoing interoperability testing
Chrome 11	April 2011			Beta Preview Release
Chrome 12	April 2011			Developer Preview Release

3.5.3.2 Microsoft Internet Explorer

Internet Explorer 7 (IE7) can continue to be used on Windows XP systems until Windows XP is retired in October 2013. The NASA System Configuration Baseline must be used for IE7.

Internet Explorer 8 (IE8) remains the preferred version of Internet Explorer for systems running Windows XP. The NASA System Configuration Baseline must be used for IE8

Interoperability testing has been completed and the remaining incompatible web application issues are being addressed. Internet Explorer 9 (IE9) will replace IE 8 as the default browser beginning February 2012 on all interoperable Windows 7 systems. IE9 is not available to systems running Windows XP. IE8 shall be removed from all Windows systems by July 2012.

3.5.3.3 Mozilla Firefox

Firefox 5 is the standard for Windows, Macintosh and Linux systems. Firefox 3 must be removed from all systems by October 1, 2011. Mozilla plans to release Firefox 6 and Firefox 7 all in calendar year 2011. Maintaining interoperability will depend on agile adoption of the latest version. Mozilla has been continuing to provide security patches for older versions of their browser, including Firefox 3.5, but have not committed to maintaining such support.

3.5.3.4 Apple Safari

Safari 5 is the standard for all interoperable Macintosh systems. Apple released Safari 5 to address security vulnerabilities present in Safari 4. Safari 4 must be removed from the environment by August 1, 2011. Safari 5.0.5 or later must be installed.

The use of Safari on Windows is not supported.

3.5.3.5 Google Chrome

Google Chrome is quickly becoming a popular browser within the industry and has been undergoing interoperability testing. At this time there are not enough unique features within Google Chrome to justify replacing Mozilla Firefox as the alternative open software browser. The use of Google Chrome is not supported within the NASA environment.

3.5.4 System Configuration Reporting and Patch Management

The Agency is transitioning to Dell KACE for patch management, compliance reporting, and system configuration reporting. The previous product, Patchlink, will be used until the new patch and configuration reporting solution is completely implemented. For current information on the appropriate configuration and patch management client for your system(s), including specific version levels, please refer to the Agency Security Update Service (ASUS) web site at:

https://asus.nasa.gov/portal

Agency policy requires that an ASUS reporting client be installed on all systems for which clients are available.

3.5.5 Desktop Encryption

3.5.5.1 Data at Rest (DAR) Encryption

NASA will continue to maintain and support McAfee Endpoint Encryption on all Windows systems identified during the Data at Rest (DAR) Implementation project. This software is compliant with federally mandated requirements for encryption of sensitive data on mobile devices (specifically laptops and removable media) and remains the Agency solution for meeting these requirements. All laptops, all desktops with Personally Identifiable Information (PII) or other similarly sensitive data[23], and all new and refreshed computers are required to implement this encryption technology. The first phase of the implementation focuses on laptops and system containing PII data. The scope and schedule varies by Center and will be revisited

23 e.g. ITAR, SBU

once the Agency Consolidated End-User Services (ACES) contract is underway. Please contact your local DAR representative for center specific deployment details or visit

https://www.odin.lmit.com/portal/dataatrest.html

for more information.

While a Mac client is available from McAfee, a pending infrastructure upgrade is required to support this client. In the interim, the use of FileVault is permitted on Apple systems.

3.5.5.2 Content Encryption and Secure Email

NASA maintains a secure desktop solution based on Entrust. The Client Reference Configurations include the appropriate Entrust client for use in encrypting desktop files and folders and Outlook plug-in sending signed, encrypting messages to other NASA employees. Work is constantly underway to extend trust to other Federal Agencies so that secure mail can be exchanged outside of NASA in the future.

For situations in which Entrust cannot be used to exchange secure files or messages, the Free Software Foundation's, GNU Privacy Guard (GnuPG) is approved for use and has been added to Table 4.1.1 Table of Optional Software. Note that GnuPG does not meet the rigorous enrollment and certificate management processes inherent with Entrust and cannot provide the authentication assurance levels necessary to meet Federal Government requirements for the exchange of sensitive information. It should therefore only be used as a point solution when Entrust is not an option.

3.6 Desktop ICAM Integration Configuration Requirements

The Identity, Credential and Access Management infrastructure services provide a significant portion of the core NASA operating environment. For proper interoperability with the ICAM services the following additional requirements have been identified.

3.6.1 Authentication Configuration Requirements

The ICAM Desktop Integration team develops software and configuration requirements for authentication with NASA standard operating systems. These configurations support such functions as:

- Smartcard PIV authentication with the NASA badge
- NASA Launchpad Simplified Logon
- Single-Sign-On with Active Directory integrated applications such as SharePoint

Desktop ICAM Integration configuration requirements, which includes settings for operating system, browser, and middleware can be found at

https://etads.nasa.gov/DII/CR

3.6.2 NASA Client Trust Reference

The NASA Client Trust Reference (NCTR) repository can be found on the ETADS web site at:

http://etads.nasa.gov/DCS/ClientTrustReference.shtml.

Trusted Sites and Certificates are listed in the NCTR when they are approved for deployment on NASA end user systems as required to enable Agency level business functions for groups of personnel appreciably larger than those at any single NASA center.

3.6.2.1 Trusted Sites

The trusted site listing facilitates secure workstation interoperability with applications and services that are both internally and externally provided.

3.6.2.2 Certificates

Operating systems, as well as some third party applications, such as Mozilla Firefox and Mozilla Thunderbird, contain trusted certificate stores. The certificate stores are already preloaded and updated periodically by the product vendors with trusted certificates that are required for standard business functionality. In addition to these vendor-supplied certificates, some of these certificate stores require additional certificates for interoperability with Agency and Agency affiliate services. This collection of additional certificates is managed as part of the NASA Client Trust Reference.

3.6.3 Additional Relying Party Requirements

All client applications that perform PKI operations shall be required to support the SHA-2 family hashing algorithms by November 2010. Information on SHA-2, RSA, and encryption algorithm lifetimes can be found in NIST special publications SP800-78-2 and SP800-131.

3.7 Electronic forms

In 2009 the Agency-wide eForms software (FileNet v4.2), used for over 16 years, was decommissioned by the vendor (IBM). The NASA OCIO is taking the necessary steps to replace the software with a new Agency-wide integrated solution that supports NASA's business practices, embraces technology and innovation, and increases efficiency.

In the interim interoperability issues may be encountered by some users. The NASA Electronic Forms Working Group is currently performing integration testing with new software option to ensure challenges are identified and workarounds, when needed, are established and communicated. Contact the working group to report issues or for more information. Contact information can be found on the NASA Electronic Forms System (NEFS) website www.nefs.nasa.gov

The NEFS web site was designed to serve as the central repository for forms used within NASA and is available to NASA Centers and Installations, recognized partners, qualified contractors/service providers, and the general public when doing business with NASA. For the purpose of form distribution, an Agency distribution center profile has been created to allow access to Agency forms. All forms users should have the NEFS distribution center profile, in addition to all of the profiles established for access to center specific, and contractor maintained form collections. These profiles are maintained and distributed through the NEFS web site

Agency-level forms (created when the subject matter of the data collection tool applies to 2 or more Centers) shall be designed through the NASA Forms Mgmt Office, and include unique a form number and edition date. Center unique versions of these agency forms should not be created or used without an approved waiver request. Center-level forms shall be designed through the Center Forms Management Office, include a unique form number and an edition date.

3.8 Section 508 Compliance Requirements

Software products procured after June 21, 2001 must be in conformance with Section 508 of the Rehabilitation Act. Complete information and guidance on addressing Section 508 requirements is available at:

http://www.nasa.gov/accessibility/section508/sec508_overview.html

When developing and testing software, users are reminded to use the recommended tools for evaluation:

3.8.1 Section 508 Tools Table

Function	Windows	Mac OS X	Linux
Screen Reading Software	JAWS 8.x or higher	VoiceOver	
	Window Eyes 6.x or higher		
Desktop Automated Tool	HiSoftware ACCVerify Deque Ramp	Deque Ramp	
PDF Documents	Adobe Acrobat 8.x or higher	Adobe Acrobat 8.x or higher	
	NetCentric Technologies CommonLook Plug-in for Acrobat		

The NASA Emerging Technologies and Desktop Standards team has evaluated vendor-supplied Voluntary Product Accessibility Templates (VPAT) for Windows XP, Windows Vista, Windows 7, Mac OS X Snow Leopard, Office 2007, and Firefox 3.6.x, and believes that they satisfy the Section 508 requirements to an acceptable degree.

3.9 FIPS 140-2 Compliance Requirements

NASA will adhere to the guidelines and recommendations of the National Institute of Standards and Technology as required by the Federal Information Security Management Act, particularly as they apply to computer security and encryption technology for desktop hardware and software. More specifically, NASA will comply with Federal Information Processing Standards (FIPS) 140-1 and 140-2 as applicable, validated encryption modules become available.

NASA application developers and service providers are reminded that whenever cryptographic-based security systems are used to protect sensitive information in computer systems, the cryptographic modules utilized must be FIPS 140-2 compliant as validated by NIST[24]. A current list of validated products can be found at:

http://csrc.nist.gov/cryptval/

The following products mentioned in NASA-STD-2804 have been validated by a NIST-accredited testing laboratory and may be appropriate to protect sensitive information with cryptography under specific conditions:

Product	Validation Module	Certification	Comments
Apple FileVault, Safari, Mail	Apple FIPS Cryptographic Module	#1514	Single User Mode, FIPS 140-2

24 Federal Information Processing Standards Publication 140-2, *Security Requirements for Cryptographic Modules*

Product	Validation Module	Certification	Comments
Microsoft	Kernel Mode Cryptographic Module for Windows XP	#997	Single User Mode, FIPS 140-1
Microsoft	Microsoft Windows 7 Cryptographic Primitives Library	#1329	Single User Mode, FIPS 140-2
Microsoft	Windows 7 Enhanced Cryptographic Provider (RSAENH)	#1330	Single User Mode, FIPS 140-2
Microsoft	Windows 7 Enhanced DSS and Diffie-Hellman Cryptographic Provider (DSSENH)	#1331	Single User Mode, FIPS 140-2
Microsoft Outlook	Outlook Cryptographic Provider	#110	Single User Mode, FIPS 140-1, S/MIME
Entrust PKI Software	Entrust Entelligence Kernel Mode Cryptographic module	#1043	Single User Mode, FIPS 140-2
F-Secure SSH	F-Secure® Cryptographic Library™ for Windows	#437	FIPS 140-2, When operated in FIPS Mode, Single User Mode.
F-Secure SSH	F-Secure® Cryptographic Library™ for Linux	#776	FIPS 140-2, When operated in FIPS Mode, Single User Mode.
OpenSSL	OpenSSL FIPS Object Module (1.2)	#1111	Single User Mode, FIPS 140-2
Citrix ICA Client for Windows	Kernel Mode Cryptographic Module for Windows XP	Not Validated	Uses MS Windows FIPS Crypto Module
McAfee Endpoint Encryption for PCs Client	Diffie-Hellman	#1131	FIPS 140-2, When operated in FIPS Mode
Mozilla NSS	Network Security Services (NSS)	#1280	FIPS 140-2, When operated in FIPS Mode
Entrust PKI Software	L Version 8.0	#797 #1043	FIPS 140-2, When operated in FIPS Mode

3.10 Wireless Requirements

The current minimum wireless hardware and software configuration that will be used by NASA to support interoperability is defined in NASA-STD-2850.1. For information on the ongoing conditions that wireless infrastructure devices must satisfy to connect to the NASA network see NASA-STD-2850.1 which when posted will be available at:

http://standards.nasa.gov/.

3.11 Internet Protocol version 6 (IPv6) Requirements

Internet Protocol version 6 (IPv6) is a new version of the Internet Protocol, designed as the successor to Internet Protocol version 4 (IPv4). IPv6 is described in Internet standard document RFC2460.

http://tools.ietf.org/html/rfc2460

Most modern day operating systems are IPv6 capable. On Windows systems from Windows Vista onward Microsoft has enabled IPv6 by default. Apple has delivered IPv6 capable systems since OS X 10.2.

To comply with Federal requirements for IPv6 capable operating systems IPv6 shall not be disabled.

3.12 Energy Management

In order to comply with Executive Order 13423, printers, laptops and desktop systems must be configured to use energy-saving settings.

3.12.1 Computers

Requirements:

- Displays shall be set to sleep after 15 minutes of idle time
- Systems shall go to sleep after 60 minutes of idle time

Wake-on-LAN functionality may be useful for administrators to wake the systems in order to perform maintenance.

Generally, the level of sleep should be as effective as possible at saving power, given the constraints of the environment. To reduce power consumption to a minimum the S4[25] power savings mode (hibernate state) shall be used.

Servers and other special-purpose systems are exempted from this requirement.

3.12.2 Printers

All clients shall be configured for duplex printing by default.

3.13 Virtualization

Virtualization technology allows multiple operating systems to be run on a single physical computer. If a desktop virtualization product is required for interoperability the recommended solution (VMWare) must be used. See Table of Optional Software. The virus protection software listed in the Client Reference Configuration shall be used with Virtualization products.

3.14 Password Management Tool

As part of the Federal and Agency Identity Credential and Access Management (ICAM) programs, NASA is implementing strong authentication for access to NASA IT systems and applications per the guidance of HSPD-12 and OMB M-11-11 using federally issued PIV smartcards, and eventually PIV-I smartcards provided by authorized issuers. Part of the strategy includes requiring system and application authentication to utilize the central authentication sources, namely the NASA Consolidated Active Directory environment and the NASA Access Launchpad for web application authentication, and to deprecate the use of single factor authentication credentials, namely username and password. While significant progress has been made, smartcard enablement is still being developed in a number of cases. Further, it is recognized that users require access to a wide array of both Federal and non-Federal IT systems, most outside of NASA's control, which employ password-based authentication mechanisms.

NIST SP 800-63 does not permit local storage of password credentials as such action would reveal the authentication secret to a party (application) other than the claimant (the user) or the verifier operated by the Credential Service Provider (the Federal IT system being accessed). Under no circumstances, shall a smartcard holder's PIV smartcard PIN, or other

25http://msdn.microsoft.com/en-us/library/ff564575.aspx

Federal IT system credentials (including NASA issued RSA token PINs, NCAD account password, and Access Launchpad password), be managed within a consumer retail or other password management tool. For access to non-Federally controlled IT systems, a password management tool is permissible if it has an implementation that is compliant with NPR 2810.1A requirements.

4 ADDITIONAL SOFTWARE TABLES

4.1 Optional Software

The following table contains optional useful functionality that is not required for interoperability. These software applications and utilities can be made available to end users upon request or distributed with standard enterprise images to support interoperability. Where practical, it is recommended that these tools be used rather than similar tools that address the same function. This table often identifies software that may be eventually be included in the Client Reference Configurations.

4.1.1 Table of Optional Software

Function	Windows	Mac OS X	Linux
3279 client	QWS3270	tn3270	tn3270
ssh client	XWin32	bundled	bundled or OpenSSH
sftp client	FileZilla	Cyberduck	bundled or OpenSSH
Advance file archive extractor/creator	WinZip 12	bundled	bundled
Real A/V Player	RealPlayer 11	RealPlayer 11	RealPlayer 11
Remote access to Windows systems	MS Remote Desktop Connection	MS Remote Desktop Connection	bundled
X window system server	XWin32	Apple X11	bundled
PostScript previewer	Ghostscript	bundled	bundled
Firefox ICAM Configuration	NASA Firefox Configuration Extension (NFCE)	NASA Firefox Configuration Extension (NFCE)	NASA Firefox Configuration Extension (NFCE)
PDF creator	Adobe Acrobat, Pro	Adobe Acrobat Pro	Scribus
PDF writer/converter	PrimoPDF, MS Office 2007 PDF plug-ins	bundled	bundled
Project Management	MS Project 2007	OpenProj	OpenProj
Alternate Cryptographic Software	Gpg4win	GPGTools	GnuPG
Virtualization	VMWare Workstation	VMWare Fusion	VMWare Workstation
Microbloggin/Twitter	TweetDeck	Nambu	Pidgin
Password Management	1Pasword	1Password	
RSS Reader			

4.2 Agency Required Software

The following table summarizes software that must be installed on all Agency desktop systems, regardless of their interoperability requirements.

This software is included in the Client Reference Configuration.

4.2.1 Agency Required Software Table

Function	Windows	Mac OS X	Linux	Unix
FISMA compliance	FDCC/NASA System Configuration Baselines	CIS Benchmarks	CIS Benchmarks	CIS Benchmarks
Patch reporting	KACE KBOX	KACE KBOX	KACE KBOX	KACE KBOX
Anti-Virus	Symantec Endpoint Protection	Symantec Anti-Virus Enterprise Edition	Symantec	Symantec
FIPS 201 Authentication	ActivClient	Bundled with OS	ActivClient	ActivClient

5 REVIEW AND REPORTING REQUIREMENTS

5.1 Interoperability Maintenance Reporting

Upon request, Center CIOs will provide the NASA CIO with a summary report, outlining the status of minimum interoperability access for each NASA employee.

5.2 Interoperability Reporting

Each Center CIO will utilize the Agency selected processes and tools, both manual and automated, to report on an annual basis to the NASA CIO the hardware and software configuration of all workstations at their respective Centers. The report will contain sufficient information to ascertain if each workstation supports NASA employees or is Government-furnished equipment to a contractor, whether the equipment is required to be interoperable, and a description of the hardware architecture/environment. The report will specify the number of NASA employees that do not have access to interoperable workstations.

5.3 Basic Interoperability Standards Maintenance

This standard, and its companion, NASA-STD-2805 Minimum Hardware Configurations, are maintained on behalf of the NASA CIO by the Emerging Technology and Desktop Standards group. Together, these standards define the software, hardware, and configurations necessary to ensure basic interoperability within the NASA information technology computing infrastructure.

This standard will be reviewed and updated on an as-required basis, not to exceed 12-month intervals. Participation in the revision process is open to all NASA employees. Details on how to be alerted of changes to the standards and/or comment on proposed updates can be found at:

http://etads.nasa.gov/

This site also maintains interim guidance, position papers, software and hardware reviews, recommendations and other documentation intended to promote standardized basic interoperability.

6 DURATION

6.1 Duration

This standard will remain in effect until canceled or modified by the NASA CIO.

7 SUPPORTING DOCUMENTS

7.1 Supporting Documents

Supporting documents and additional information related to this standard may be found at:

http://etads.nasa.gov/DCS